Maurer School of Law: Indiana University
Digital Repository @ Maurer Law

Indiana Journal of Global Legal Studies

Volume 26 | Issue 2 Article 11

Summer 8-1-2019

Defining Critical Infrastructure for a Global Application

Colleen M. Newbill
Indiana University Maurer School of Law, cnewbill@iu.edu

Defining Critical Infrastructure for a Global Application

COLLEEN M. NEWBILL*

ABSTRACT

A Google search for the phrase "critical infrastructure" turns up 189 million results in little more than a half second: "global critical infrastructure" has 151 million results; and "definition of critical infrastructure" yields 71.5 million results. The list of what industries and sectors fall under the critical infrastructure designation expands as time progresses and technology develops. As the threat of cyberattacks increases and this frontier of terrorism continues to emerge, attacks on critical infrastructure are high on the list of concerns and the need for protective measures imperative. The focus on protecting critical infrastructure does not stop at the borders of individual nation-states as calls for international efforts to protect national critical infrastructures are being made. Without clearly defined boundaries on what constitutes critical infrastructure at a global level, however, international efforts to protect critical infrastructure will be unduly burdensome and overbroad. Before moving toward international efforts for protecting critical infrastructure, the global community must come together to define which critical infrastructures are worth this additional level of protection.

INTRODUCTION

The last decade has seen the rise of the nation-state as a malicious actor in cyberspace. The lone hacker or activist group perpetrating cyber-vandalism or theft is no longer the image of an enemy on the other side of the screen when addressing cybersecurity. The threat now

* J.D. Candidate, 2019, Indiana University Maurer School of Law—Bloomington; M.S. Candidate in Cybersecurity Risk Management, 2019, Indiana University—Bloomington; B.A. in Linguistics, 2010, Indiana University—Bloomington. I would like to thank Professor Fred Cate, whose class lectures inspired this note. I would also like to thank those friends and family who provided comments and editing assistance while I drafted this note.

Indiana Journal of Global Legal Studies Vol. 26 #2 (Spring 2019)

lies in state-sponsored hacking and cyberattacks. In 2010, the United States and Israel launched a computer worm that damaged centrifuges used to purify uranium in Iranian nuclear facilities.[1] Four years later, in an unprecedented move of charging state actors from another country, the U.S. Department of Justice filed indictments against five members of the People's Liberation Army for "computer hacking, economic espionage and other offenses" conducted against U.S. companies in various industries, including nuclear power plants and energy companies.[2] The following year, North Korea was identified as the party behind the cyberattack on Sony Pictures, where hackers stole confidential data and subsequently released the information online.[3] Nation-state actors have launched attacks against both civilian and military targets via cyberspace, making an already challenging situation worse.

In February 2017, Brad Smith, president of Microsoft, gave the keynote address at the Rivest, Shamir, and Adleman Conference in San Francisco, California. The topic of his address was the problem of cybersecurity and the need for new solutions.[4] One of the major complications in creating new solutions is this new role of the nation-state actor as a threat and not a target.[5] Cyberspace is the new frontline of battle, but unlike prior battlefields that progressed from land to sea to air,[6] cyberspace is not a physical place.[7] Furthermore, cyberspace is not a sovereign territory that is protected by borders under the authority of the nation-state, but is rather often controlled by the private sector.[8] The premise of Smith's address is that this new frontline has nation-states attacking civilians and the private sectors rather than other government actors, and because of this shift, civilians are often

1. David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES (June 1, 2012), http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=1&_r=1&hp.

2. Press Release, DEP'T OF JUSTICE, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor; *see also* Evan Perez & Shimon Prokupecz, *U.S. Plans to Publicly Blame Iran for Dam Cyber Breach*, CNN (Mar. 10, 2016, 5:35 PM), http://www.cnn.com/2016/03/10/politics/iran-us-dam-cyber-attack/index.html.

3. Perez & Prokupecz, *supra* note 2; *see also* Kim Zetter, *Sony Got Hacked Hard*, WIRED (Dec. 3, 2014, 4:02 PM), https://www.wired.com/2014/12/sony-hack-what-we-know/.

4. Brad Smith, President and Chief Legal Officer, Microsoft, Keynote Address at the RSA Conference: The Need for a Digital Geneva Convention (Feb. 14, 2017).

5. *Id.*

6. *Id.*

7. *Id.*

8. *Id.*

the first responders.[9] Smith calls for the world's governments to come together to protect civilians like they did when the Geneva Conventions of 1949 were drafted.[10] Unlike the Geneva Conventions that were established to protect civilians during times of war, however, Smith believes the world's governments need to unite to protect civilians on the Internet in times of peace.[11]

Smith proposes the creation of a "Digital Geneva Convention" to ensure civilian protection on the internet and in cyberspace during times of peace; he calls for world governments to pledge not to engage in specific behaviors that threaten civilians and to work together with the private sector to respond to threats that do occur.[12] The proposal lays out six objectives: (1) "no targeting of tech companies, private sector, or critical infrastructure"; (2) "assist private sector efforts to detect, contain, respond to, and recover from" cyberattacks; (3) "report vulnerabilities to vendors"; (4) "exercise restraint in developing cyber weapons"; (5) "commit to nonproliferation activities to cyberweapons"; and (6) "limit offensive operation."[13] The purpose of these objectives is that, under such a convention, the world's governments "will not target civilian infrastructure, whether it's of the electrical or the economic or the political variety."[14]

This proposal is not the only call for international action to address this threat.[15] As nation-states continue to threaten the cybersecurity of

---

9. *Id.*
10. *Id.*
11. *Id.*
12. *Id.*
13. *Id.*
14. *Id.*
15. In November 2018, at the UNESCO Internet Governance Forum, French President Emmanuel Macron announced an international initiative between more than fifty countries, ninety nonprofit groups and universities, and over a hundred corporations. Louise Matsakis, *The U.S. Sits Out an International Cybersecurity Agreement*, WIRED (Nov. 12, 2018, 7:37 PM), https://www.wired.com/story/paris-call-cybersecurity-united-states-microsoft/. The Paris Call for Trust and Security in Cyberspace has been described as being "akin to a Geneva Convention for the digital world." *Id.* In the agreement, the signatories have affirmed a "willingness to work together . . . and to assist on another" to (1) "Prevent and recover from malicious cyber activities that threaten or cause significant, indiscriminate or systemic harm to individuals and critical infrastructure;" (2) "Prevent activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet;" (3) "Strengthen our capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities;" (4) "Prevent ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sector;" (5) "Develop ways to prevent the proliferation of malicious ICT tools and practices intended to cause harm;" (6) "Strengthen the security of digital processes, products and services, throughout their lifecycle and

both civilians and other nation-states, calls for a convention or agreement between world governments will increase.[16] However, the idea of a Digital Geneva Convention stipulating behaviors to be adhered to during times of peace is not without its issues. It may create new vulnerabilities in national security or encroach on nation-state sovereignty, but those concerns are outside the scope of this note. This note takes a closer look at the proposal's first principle and focuses on the idea of protecting critical infrastructure within the bounds of a potential Digital Geneva Convention. While the general principle of what constitutes critical infrastructure is similar across borders, there is not a single, global definition. For a Digital Geneva Convention to be effective, there must be some degree of global uniformity as to what constitutes critical infrastructure. Because the priorities of different countries can vary as to what is considered critical, a second definition for critical infrastructure is necessary.

The purpose of this note is to address the need for and propose a second definition of critical infrastructure in an application such as a Digital Geneva Convention. Part two of this note will address how critical infrastructure has been defined historically and in the physical world. It will also look at the Geneva Conventions of 1949 and how they

---

supply chain;" (7) "Support efforts to strengthen an advanced cyber hygiene for all actors;" (8) "Take steps to prevent non-State actors, including the private sector, from hacking-back, for their own purposes or those of other non-State actors;" and (9) "Promote the widespread acceptance and implementation of international norms of responsible behavior as well as confidence-building measures in cyberspace." Paris Call for Trust and Security in Cyberspace, Nov. 12, 2018, https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf. These goals map onto the principles outlined by Brad Smith, but like his proposal, there are no explicitly defined terms to make these goals a reality. While the Paris Call is one of the first steps toward international efforts in cybersecurity, the lack of concrete terms highlights why constructing a global definition for critical infrastructure is necessary.

16. *See generally* Rihards Kols, *Cyberspace Needs Its Own 'Geneva Convention'*, RIHARDS KOLS (Sept. 20, 2017), http://www.rihardskols.lv/r-kols-cyberspace-needs-its-own-geneva-convention/ (explaining the need for international cooperation in addressing cyberspace as a new military sphere); Jovan Kurbalija, *Digital Geneva Convention: Multilateral Treaty, Multistaker Implementation*, HUFFINGTON POST (Feb. 27, 2017, 10:35 AM), https://www.huffingtonpost.com/entry/digital-geneva-convention-multilateral-treaty-multistakeholder_us_58b443c0e4b02f3f81e44a35 (discussing Brad Smith's proposal for a digital Geneva Convention and its implementation); Teri Robinson, *A Cyber Geneva Convention*, SC MEDIA (May 1, 2017), https://www.scmagazine.com/home/security-news/features/a-cyber-geneva-convention/ (analyzing Brad Smith's proposal within the context of the rules of engagement). *But see* Jonathon Keane, *A Digital Geneva Convention Will Only Go So Far*, PASTE (May 19, 2017, 9:00 AM), https://www.pastemagazine.com/articles/2017/05/a-digital-geneva-convention-for-cybercrime-will-on.html (discussing the international agreements already in existence to govern cyberspace and the need for an independent body to enforce and investigate violations of a digital Geneva Convention).

applied to infrastructure to protect civilians. Next, part three will look at how modern critical infrastructure has been defined and how the rise of the internet and networking systems together has affected the definition. Finally, part four will propose a global definition of critical infrastructure and what underlying criteria should be considered.

HISTORY OF CRITICAL INFRASTRUCTURE AND THE GENEVA CONVENTIONS OF 1949

While the term "critical infrastructure" may not have been used to describe systems vital to a nation's functioning, such systems have always been in place. The protection and targeting of these systems are often viewed from a national security perspective and how they affect the nation-state's ability to function. Critical infrastructure, whether by that name or another, however, has served civilians first and foremost.

A Brief History of Critical Infrastructure and Its Role from Civilian and Military Perspectives

Critical infrastructure dates as far back as ancient Rome and Greece. The Roman Empire has been recognized throughout history for its road systems, food stores, and aqueducts.[17] Rome's aqueducts were "critical to ancient Roman civilization and its evolution from a regional power into a vast empire."[18] These systems were deemed "indispensable"[19] and as such were protected and hidden to protect the Roman water system from external threats.[20] While the aqueducts were made to serve the civilian population, they were also an advantage militarily and thus a target for attacking forces. When Rome began to build the aqueducts above ground, the purpose of the infrastructure changed from being "a hidden and purpose-build system that delivered an essential service into a 'visible' symbol of greatness through the use of technology."[21] This shift in purpose, however, made the water system's infrastructure vulnerable. These systems were then exploited by Rome's enemies, and the water supply was disrupted until eventually, the only aqueducts left were the original, underground

17. Michael J. Assante, Idaho Nat'l Lab., Proceedings of the 42nd Hawaii International Conference on System Sciences: Infrastructure Protection in the Ancient World 1 (Jan. 5, 2009), http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.401.7316&rep=rep1&type=pdf.

18. *Id.*

19. *Id.* at 2.

20. *Id.* at 3.

21. *Id.*

aqueducts.[22]

Often an opposing force attacks a critical infrastructure to weaken not only the military forces but also the general population as well. For example, the seizure of Hellespont, the source of grain imports for Athens in ancient Greece, resulted in the starvation of the city and Athens' subsequent defeat at Aegospotami.[23] To protect Hellespont, Athens sent over thirty-five thousand men to prevent the strait from being closed and the grain from being seized.[24]

Food and water supplies are not the only early forms of critical infrastructure that were targeted. Means of transportation were also often targeted. During World War II, the Allied forces bombed Germany's railway system, which ultimately halted the delivery of goods and brought the German economy to the brink of collapsing.[25] Attacks on vital systems go far beyond affecting a nation's government or military operations and often have devastating effects on civilian populations.

The Geneva Conventions of 1949 and Protecting Civilians in Times of War

In August 1949, the four Geneva Conventions were signed by eighteen government delegations.[26] As of the early 2000s, 194 nation-states had become parties to the Geneva Conventions.[27] These conventions were created and ratified after World War II in response to the violent acts committed against victims and civilians during the war.[28] Philip Spoerri, International Committee of the Red Cross Director for International Law and Cooperation, stated in his address commemorating the sixtieth anniversary of the 1949 Geneva Conventions that the "basic notion underlying the Geneva Conventions

---

22. *Id.* at 3-4.

23. *See* KATHI ANN BROWN, CRITICAL PATH: A BRIEF HISTORY OF CRITICAL INFRASTRUCTURE PROTECTION IN THE UNITED STATES, at xiv (2006) (reviewing the history of the Spartan capture of Hellespont).

24. *See generally* JOHN R. HALE, LORDS OF THE SEA (2009) (explaining the story of Sparta's attack on Hellespont in Greek history).

25. BROWN, *supra* note 23, at xiv-xv.

26. *See* Philip Spoerri, Director of International Law, ICRC, The Geneva Conventions of 1949: Origins and Current Significance (Dec. 8, 2009), https://www.icrc.org/eng/resources/documents/statement/geneva-conventions-statement-120809.htm.

27. *Id.; see also Treaties, State Parties and Commentaries*, ICRC (last visited Nov. 10, 2018), https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/States.xsp?xp_treatySelected=380&xp_viewStates=XPages_NORMStatesParties.

28. *See* Spoerri, *supra* note 26.

is the notion of respect for the life and dignity of the individual."[29]

The Fourth Geneva Convention (Convention IV) specifically deals with the treatment of civilians during times of war and provides regulations for the general security of populations and protected persons.[30] The idea of respect for the life and dignity of the individual is reflected in Part I of Convention IV; it prohibits distinctions in treatment based on "race, colour, religion or faith, sex, birth or wealth," "violence to life and person," "taking of hostages," behaviors that degrade personal dignity, and extrajudicial sentences and executions.[31] Convention IV focuses more on the protection of human rights for civilians during war rather than attempting to ban violence against civilians.

Additional protections for civilians were granted through the Protocols Additional to the Geneva Convention in 1977 (the Additional Protocols).[32] Part IV of the Additional Protocols discusses rules related to the civilian population.[33] While the Additional Protocols continue to focus on human rights, Part IV also explicitly addresses the use of force. Article 49 of the Additional Protocols defines an attack as "acts of violence against the adversary, whether in offense or in defense."[34] It prohibits "[a]cts or threats of violence the primary purpose of which is to spread terror among the civilian population . . . ."[35]

The Additional Protocols further deem any attack "which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated" as indiscriminate.[36] While the definition of an attack is accepted international law, some legal scholars have suggested that an act must inflict harm to be considered an attack.[37] This idea is supplemented by the Additional Protocols' prohibited attacks. These rules are "necessarily ill-defined and 'no objective standards exist as to

---

29. *Id.*

30. *See generally* Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 75 U.N.T.S. 287 (detailing the limits of warfare in order to protect civilians during times of war) [hereinafter Fourth Geneva Convention].

31. *Id.* art. 3.

32. *See generally* Protocols Additional to the Geneva Conventions, Aug. 12, 1949 (extending additional protections to civilians and protected people during times of war) [hereinafter Protocols].

33. *See generally id.* pt. IV (describing the protections granted specifically to civilian populations).

34. *Id.* art. 49.

35. *Id.* art. 51, cl. 2.

36. *Id.* art. 51, cl. 5(b).

37. Sasha Romanosky & Zackary Goldman, *Understanding Cyber Collateral Damage*, 9 J. NAT'L SECURITY L. & POL'Y 233, 241 (2017).

where this turning point lies;' determinations are by necessity fact-bound."[38]

Both Convention IV and the Additional Protocols protect civilian systems and places. Although "critical infrastructure" is not found within the four corners of either document, there are regulations pertaining to the protection of civilian hospitals;[39] medical transport;[40] and passage of medical supplies, food, and clothing.[41] The Additional Protocols bar attacks on "civilian objects," which further added protections for locations that civilians are likely to frequent, such as places of worship and schools.[42] Article 54 explicitly prohibits targeting and destroying "objects indispensable to the survival of the civilian population," such as water systems and agricultural areas.[43] Finally, the Additional Protocols include protections of those systems that, if destroyed, would likely cause severe loss to the civilian population.[44] These include military installations and dams, which are protected if their destruction would release "dangerous forces" that would negatively affect civilians.[45] These civilian systems and places have been incorporated into what are now deemed "critical infrastructures" of many nation-states.

MODERN CRITICAL INFRASTRUCTURE AND THE DIGITAL LANDSCAPE

Modern Definitions of and Approaches to Critical Infrastructures

From the earliest societies establishing roads and governments to the modern idea of interdependent utilities and financial systems, what constitutes a country's critical infrastructure changes as society's needs shift and technology advances.[46] Modern definitions of what systems constitute critical infrastructure ultimately vary little from one nation-state to another, but the prioritization within each system may differ greatly. It has been noted that "[c]omponents of one infrastructure . . . can differ markedly in their criticality to the survival of the overall system"[47]; thus, non-essential systems are incorporated into the critical

38. *Id.*
39. Fourth Geneva Convention, *supra* note 30 at art. 18.
40. *Id.* art. 21-22.
41. *Id.* art. 23.
42. Protocols, *supra* note 32, art. 52.
43. *Id.* art. 54.
44. *Id.* art. 56.
45. *Id.* art. 56, cl. 1.
46. *See generally* BROWN, *supra* note 23 (detailing the history of critical infrastructure in the United States).
47. *Id.* at 9.

infrastructure while excluding some vital sectors. How nation-states define and prioritize these systems is critical to creating a globally applicable definition of critical infrastructure.

U.S. policy defined critical infrastructure for the first time in 1996.[48] In Executive Order 13010, President Bill Clinton stated that certain national infrastructures were "so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States" and established a commission to develop a strategy to protect such systems from attack.[49] The Executive Order then categorizes the potential threats, stating "[t]hreats to these critical infrastructures fall into two categories: physical threats to tangible property ("physical threats"), and threats of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures . . . ."[50] At that time, there were only eight sectors considered to be critical.[51]

After the terrorist attacks on September 11, 2001, the definition was expanded to include sectors outside of defense and the economy. The Critical Infrastructures Protection Act of 2001 broadened the critical infrastructure definition to include those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[52] This definition has not changed since 2001.[53] The number of vital systems since then, however, has doubled.[54] These systems, which are considered to "provide[ ] the essential services that underpin American society and serve as the backbone of our nation's economy, security, and health,"[55] are divided into sixteen sectors: (1) chemical; (2) commercial facilities; (3) communications; (4) critical manufacturing; (5) dams; (6) defense industrial base; (7) emergency services; (8) energy; (9) financial services;

---

48. *Id.*

49. Exec. Order No. 13010, 61 Fed. Reg. 37347 (July 17, 1996).

50. *Id. See also* Dorsey Wilkin, et al., *Cyberspace Policy for Critical Infrastructures, in* CRITICAL INFRASTRUCTURE PROTECTION II, at 17, 18 (Mauricio Papa & Sujeet Shenoi, eds., 2008).

51. Exec. Order No. 13010, *supra* note 49.

52. Critical Infrastructures Protection Act of 2001, 42 U.S.C. § 5195c(e) (2012).

53. *See generally* Wilkin, *supra* note 50 (detailing the progression of U.S. critical infrastructure).

54. *See* Presidential Policy Directive PPD-21 (Feb. 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

55. *What is Critical Infrastructure?*, DEP'T OF HOMELAND SEC. (Dec. 8, 2017), dhs.gov/what-critical-infrastructure.

(10) food and agriculture; (11) government facilities; (12) healthcare and public health; (13) information technology; (14) nuclear reactors, materials, and waste; (15) transportation systems; and (16) water and wastewater systems.[56]

The United Kingdom similarly defines critical infrastructure as:

> those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in: a) major detrimental impact on the availability, integrity or delivery of essential services—including those services, whose integrity, if compromised, could result in significant loss of life or casualties—taking into account significant economic or social impacts; and/or b) significant impact on national security, national defence, or the functioning of the state.[57]

Also like the United States, these elements are further divided into sectors: "chemicals, civil nuclear, communications, defence, emergency services, energy, finance, food, government, health, space, transport, and water."[58] Communications, emergency services, and transport are further divided into sub-sectors, such as broadcast, telecommunications, internet, and postal; ambulance, coastguard, fire and rescue, police, electricity, gas, and oil; and aviation, ports, rail, and road.[59]

While the United States and the United Kingdom include a wide variety of sectors in their critical infrastructure, some countries do not have such broad definitions. India, for example, lists "the sectors of power, water supply, communications, transportation, defence and finance [as] vital constituents of national security."[60] Priorities as to

---

56. Jeh Johnson, Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector, DEP'T OF HOMELAND SEC. (Jan. 6, 2017), https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical (Each of the sectors are divided into approximately twenty sub-sectors. After this note was drafted, the Department of Homeland Security designated election infrastructure as a sub-sector of government facilities, establishing such infrastructure as critical. Secretary of Homeland Security under President Obama, Jeh Johnson, stated that "Given the vital role elections play in this country, it is clear that certain systems and assets of election infrastructure meet the definition of critical infrastructure, in fact and in law.").

57. CABINET OFFICE, SUMMARY OF THE 2015-16 SECTOR RESILIENCE PLANS (2016).

58. *Id.*, at 3.

59. CABINET OFFICE, *supra* note 57, at 6.

60. IDSA TASK FORCE REPORT, INDIA'S CYBER SECURITY CHALLENGE 33 (2012).

what is critical to a nation-state's survival vary between different nation-states, and these discrepancies could lead to confusion or conflict regarding what critical infrastructure sectors warrant international protection. As threats to critical infrastructure increase in the digital world, how a country defines its vital systems will be crucial in determining how future international laws are defined and what the future rules of engagement may be.

Threats to Critical Infrastructure in Cyberspace

In 2015, the United Kingdom determined that the threat of a cyberattack on infrastructure was not likely to occur in the next five years, and should an attack take place, the impact would not have an overall catastrophic impact.[61] Attacks on physical infrastructure or transport systems were considered more probable, but the United Kingdom believed that there would be no greater impact on the country than a cyberattack.[62] Since 2015, however, there have been numerous attacks on various nation-states' infrastructures. While none have seemingly produced catastrophic results, as the number of attacks continues to increase, it is simply a matter of time before an attack will devastate a country.

Attacks on critical infrastructure in the physical world have devastated civilizations, such as the Roman Empire.[63] Nevertheless, military attacks are not the only means of affecting critical infrastructure. Civil emergencies affecting a country's critical infrastructure can stem from accidents—such as technical failures or natural disasters. If a technical failure occurs in vital sectors, damage can be catastrophic and cause widespread destruction and hundreds of deaths. This occurred with the Malpasset dam failure in southern France in 1959 that destroyed two small villages and killed over four hundred people.[64] While this was a technical failure of the dam due to physical vulnerabilities, one can imagine how a cyberattack on a country's dam system might play out. In 2013 a cyberattack on a New York dam managed to access office systems rather than the operational systems of the dam.[65] Despite the attack's failure to cause any

61. *See* CABINET OFFICE, NATIONAL RISK REGISTER OF CIVIL EMERGENCIES 12 (2015) [hereinafter Register of Civil Emergencies].

62. *Id.*

63. *See supra* Part II.

64. REGISTER OF CIVIL EMERGENCIES, *supra* note 61, at 35.

65. *See* John Bonazzo, *Cyber Attack on New York Dam Highlights the Dark Side of the Internet of Things*, OBSERVER, (Mar. 10, 2016, 6:00 PM), http://observer.com/2016/03/cyber-attack-on-new-york-dam-highlights-the-dark-side-of-the-internet-of-things/; *see also*

destruction, the mere ability to gain access to any part of the system is alarming. The increase in technology being used to connect sectors within a nation's critical infrastructure increases the attack surface, as now malicious actors can "aspire to attack the national infrastructure using both traditional methods and more novel methods such as cyber-attack."[66]

In 2016, Verizon Security Solutions released a report disclosing a breach of a water company.[67] Due to the nature of the breach, Verizon opted not to disclose the name of the company nor its location but did release details about the breach.[68] By infiltrating the water company's system, hackers were able to manipulate the chemical levels in the water; however, Verizon reported that the manipulations were likely unintentional as the hackers went after the customer records.[69] While the company managed to reverse the changes before any customers were affected by the contaminated water supply, this event illuminates how easily a vital system can be affected if a motivated attacker were to infiltrate the systems.

Water supply systems are not the only infrastructure sectors that have been targeted in the last few years. Attempted attacks on London's electricity substations occurred throughout the 1990s and resulted in widespread damage and disruption.[70] These attacks have carried into the new millennium with attacks on the energy infrastructure in Algeria and Yemen.[71] These attacks were all conducted via physical intrusions until recently, as cyberattacks have become increasingly common. The best example of this is Russia's consistent attacks on the Ukrainian electrical grid over the course of the last few years.

Russia's cyber-operations against Ukraine have been perhaps the strongest indicator of a nation-state's ability to maliciously interfere

---

Perez & Prokupecz, *supra* note 2; Danny Yadron, *Iranian Hackers Infiltrated New York Dam in 2013*, WALL STREET JOURNAL, (Dec. 20, 2015, 8:49 PM), https://www.wsj.com/articles/iranian-hackers-infiltrated-new-york-dam-in-2013-1450662559?mg=prod/accounts-wsj.

66. REGISTER OF CIVIL EMERGENCIES, *supra* note 61, at 42.

67. *See generally* Mary-Ann Russon, *Hackers Hijacking Water Treatment Plant Controls Shows How Easily Civilians Could be Poisoned*, INT'L BUS. TIMES (Mar. 23, 2016, 4:35 PM), http://www.ibtimes.co.uk/hackers-hijacked-chemical-controls-water-treatment-plant-utility-company-was-using-1988-server-1551266 (detailing the cyber-attack on an unidentified water plant); Michael Hill, *Water Treatment Plant Hit by Cyber-attack*, INFO SECURITY (Mar. 24, 2016), https://www.infosecurity-magazine.com/news/water-treatment-plant-hit-by/ (discussing the system vulnerabilities that allowed hackers to infiltrate a water plant).

68. *See* Russon, *supra* note 67.

69. *See generally id.*; *see also* Hill, *supra* note 67.

70. REGISTER OF CIVIL EMERGENCIES, *supra* note 61, at 47.

71. *Id.*

with another country's critical infrastructure. Since 2014, various cyberattacks have been launched against Ukrainian industries, including energy companies, railway systems, and television broadcast stations.[72] Attacks rose in severity in December 2015 when three energy companies were infiltrated and the electrical grids were physically damaged, which left over two hundred thousand people in Ukraine without power.[73] Additionally, communication channels were disabled and security measures changed, which prevented the companies from quickly addressing the blackouts.[74] Almost exactly one year later, a second attack on Ukraine's power grid occurred.[75] During the attack, a power station was targeted, one-fifth of Kiev's electrical power was shut off, and over one hundred thousand people were without power.[76] Russia's attacks on Ukraine are not limited to the power grid; in December 2016, Ukrainian President Petro Poroshenko reported 6,500 attacks on thirty-six Ukrainian targets over a period of two months and attributed the attacks to Russia.[77] Nearly every sector has been affected by cyberattacks, including media, finance, transportation, military, politics, and energy.[78]

Attacks like these directly affect the physical world and threaten the safety and well-being of civilian populations. While the Ukrainian attacks have not resulted in extensive damage, there is concern that this is merely a prelude for larger-scale attacks. This fear is not limited to attacks by Russia. Many of these cyberattacks on infrastructure systems are thought to be testing grounds for experimenting with new methods of attacking vulnerable targets and seeing how a nation-state will respond. These attacks "can be conceived and planned without detectable logistic preparation. They can be invisibly reconnoitered, clandestinely rehearsed, and then mounted in a matter of minutes or even seconds without revealing the identity and location of the attacker."[79] As Phil Lancombe, the former staff director of the President's Commission on Critical Infrastructure Protection, has

---

72. *See generally* Scott J. Shackelford, et al., *From Russia With Love: Understanding the Russian Cyber Threat to U.S. Critical Infrastructure and What to Do About It*, 96 NEB. L. REV. 320, 324-36 (2017) (providing a brief history of the Ukraine grid hacks and the effects arising from the cyber-attacks).

73. *Id.* at 325.

74. *Id.*

75. *Id.*

76. *Id.*

77. Andy Greenberg, *How an Entire Nation Became Russia's Test Lab for Cyberwar*, WIRED (June 20, 2017, 6:00 AM), https://www.wired.com/story/russian-hackers-attack-ukraine/.

78. *Id.*

79. BROWN, *supra* note 23, at 129.

stated, if a malicious actor can find a way to attack the United States without passing the "threshold of provocation that would evoke a 'Desert Storm kind of response,'" then the United States is put "in the position of not being able to assert its own will."[80] This is not a sentiment that is limited only to the United States; it may be the position in which many countries will find themselves as attacks on critical infrastructures increase.

The International Community's Approach to Critical Infrastructure in Cyberspace

The international community has taken steps, both as individual nation-states and as a larger entity, to ensure protections from cyberattacks. In the past few years, for example, China has reached agreements with both Canada and the United States promising that neither party will commit cyber-espionage on the other.[81] But these agreements are limited to the private sector and acts of espionage for economic or intellectual property purposes.[82] While these agreements have successfully deterred economically motivated cyberattacks, [83] they are merely an important first step toward an international "rules of conduct" for cyberspace, not the final step.

Norms for critical infrastructure protection during times of peace have been proposed and adopted within the international community. Those norms that have been adopted can be a starting point to a more fully developed Digital Geneva Convention. A 2015 U.N. report found the use of information and communication technologies (ICT) in targeting "critical infrastructure and associated information systems of a State" to be a serious and real threat.[84] Furthermore, it identified the "dramatic increase in incidents involving the malicious use of ICTs by

80. *Id.* at 50.

81. *See China, Canada Vow Not to Conduct Cyber Attacks on Private Sector*, REUTERS, June 25, 2017, https://www.reuters.com/article/us-canada-china-cyber/china-canada-vow-not-to-conduct-cyber-attacks-on-private-sector-idUSKBN19H06A; *see also* Doug Olenick, *U.S.-China Cyber Agreement: Flawed, but a Step in the Right Direction*, SC MEDIA, Jan. 24, 2017, https://www.scmagazine.com/us-china-cyber-agreement-flawed-but-a-step-in-the-right-direction/article/633533/.

82. *Id.*

83. *See generally* Adam Segal, *The U.S.-China Cyber Espionage Deal One Year Later*, COUNCIL ON FOREIGN RELATIONS (Sept. 28, 2016), https://www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later (discussing the success that the United States-China Agreement has seen since implementation).

84. U.N. General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶ 5, U.N. Doc. A/70/174 (July 22, 2015) [hereinafter Report of GGE].

State and non-state actors" as a disturbing trend that creates risks for all nation-states.[85] The U.N. Group of Governmental Experts (GGE) recommended "a State should not conduct or knowingly support ICT activity that intentionally damages or otherwise impairs the use and operation of critical infrastructure."[86] The GGE report also encouraged nation-states to incorporate a "national computer emergency response team and/or cybersecurity incident response team" as a part of the critical infrastructure.[87] The report, however, does not define what constitutes critical infrastructure.

REDEFINING CRITICAL INFRASTRUCTURE FOR A GLOBAL APPLICATION

If the international community is going to take on the mantel of protecting civilians by protecting nation-states' critical infrastructures, it will need to redefine what institutions are vital to a nation-state. The "growing dependence on computer networks by critical infrastructure systems"[88] requires nation-states and the international community as a whole to determine what protections these intangible systems should be given. The "growth in the complexity of computer-based systems,"[89] which often form the backbone of the physical critical infrastructures of nation-states, has outpaced the development of security measures. These discrepancies "make[ ] these systems increasingly vulnerable to programming errors and bugs, as well as to malicious abuse and exploitation"[90] and must be addressed as a part of international norms establishing protections for critical infrastructure. The GGE report calls for potentially broadening critical infrastructures by adding "incident response team[s]"[91] to those systems vital to the functioning of a nation-state. The United States and the United Kingdom seem to follow this reasoning and have incorporated cybersecurity, while not directly into the critical infrastructure system as its own sector, as a vital part of defense.

In response to the Cyberspace Policy Review in 2009, conducted to provide a comprehensive assessment of U.S. cybersecurity policies,[92]

---

85. *Id.* ¶ 3.

86. *Id.* at 2; *see also* Shackelford, *supra* note 72 at 334.

87. Report of GGE, *supra* note 84 at 10.

88. Oren Gross, *Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-incidents*, 48 CORNELL INT'L L.J. 481, 481-83 (2015).

89. *Id.*

90. *Id.*

91. *Id.*

92. Press Release, WHITE HOUSE, President Obama Directs the National Security and Homeland Security Advisors to Conduct Immediate Cyber Security Review, (Feb. 9, 2009),

President Barack Obama stated "our digital infrastructure—the networks and computers we depend on every day—will be treated as they should be: a strategic national asset. Protecting this infrastructure will be a national security priority."[93] In 2010, "[d]uring a time of significantly reduced budgets," "the United Kingdom opted to forego the production of aircraft capable aircraft carriers and allocate those resources to expanding and maintaining its cyber defense."[94] This move further emphasized the shift of nation-states' priorities away from protecting physical systems to protecting intangible infrastructures. In 2015, the U.K. government budgeted £1.9 billion over the next five years for cyber-defense.[95]

While nation-states recognize the need to protect their critical infrastructures from cyberattacks, "budgetary constraints and resource limitations have made it impractical to protect every single asset."[96] As individual nation-states begin (or continue) to prioritize protecting their critical infrastructure through cyber-defense, international treatises and reports will continue trying to establish *cybernorms* to govern this new territory.[97] These established norms, however, ignore how norms naturally develop. The ideas for cybernorms "conceptualize norms as *products*, focusing on what norms should say rather than how they will work."[98] Establishing accepted norms does not work by defining how a group should act and then implementing them onto a society.

Norms are not deracinated abstractions; they do not come about by fiat or desire, and they are never imposed in a vacuum. Norms are social creatures that grow out of specific contexts via social processes and interactions among particular groups of actors. Understanding both those contexts and those processes is as important to successful norm construction as agreeing on content.[99]

The international community should look within these contexts and nation-state interactions for guidance in creating the new cyberspace

---

http://www.whitehouse.gov/the_press_office/advisorstoconductimmediatecybersecurityreview.

93. Eric Jensen, *Responses to the Ten Questions*, 37 WM. MITCHELL L. REV. 5049, 5050 (2011).

94. *Id.* at 5050-51.

95. NATIONAL SECURITY STRATEGY AND STRATEGIC DEFENCE AND SECURITY REVIEW, HM GOVERNMENT at 40 (2015).

96. Christine Izuakor & Richard White, *Critical Infrastructure Asset Identification*, *in* CRITICAL INFRASTRUCTURE PROTECTION X, at 27 (Mason Rice & Sujeet Shenoi, eds., 2016).

97. *See generally* Martha Finnemore & Duncan B. Hollis, *Constructing Norms for Global Cybersecurity*, 110 AM. J. INT'L L. 425, 426 (2016) (discussing the implementation of social norms in cyberspace).

98. *Id.* at 427.

99. *Id.*

norms.

These internationally determined norms, if created in a vacuum without context, will eventually conflict with nation-states' beliefs and priorities. If the international community, whether through the United Nations or another international body, continues to develop and implement cybernorms "as products,"[100] future successes may potentially be hindered by individual nation-states' competing interests and priorities.

A better solution to balancing international norms and individual sovereignty may be to establish a globally accepted definition of what constitutes critical infrastructure. A singular definition could be used in international agreements or conventions to protect civilians in both times of peace and war. Like the Protocols Additional to the Geneva Convention in 1977 banned attacks that would affect civilians by depleting food stores or destroying places of worship,[101] these new agreements could prohibit attacks on systems that are included in a global definition of critical infrastructure.

In determining what criteria would form the basis of this new definition, basic necessities should be considered, such as protecting food stores and water supplies. Additionally, the systems that aim to protect civilians from continuing harm or devastation should be included, such as emergency services. If the purpose of a global definition of critical infrastructure is to ensure civilian protections at an international level, there must be limits to what is considered vital as to not impede a nation-state's ability to wage war if necessary. Prohibiting attacks on current critical infrastructures would theoretically protect military targets, like nuclear facilities and defense. While this would be ideal, enforcement of such a bar would be nearly impossible.

Critical infrastructure at a global level should encompass systems where, if substantially or completely destroyed, the basic survival of civilians would be in peril. This single, global definition would protect critical infrastructures that are necessary and vital to the survival of civilians rather than that of a nation-state. As priorities may change for what a nation-state considers critical, expanding as technology allows and encompassing more as critical, this definition can remain static. Consider the U.S. sectors that comprise its critical infrastructures—including commercial facilities. This sector consists of eight subsectors, such as entertainment and media, gaming, and sports leagues.[102] While attacks on any of these subsectors would be devastating, and in fact

---

100. *See id.*

101. *See* Protocols, *supra* note 32; *see also supra* Part II.

102. *Commercial Facilities Sector*, DEP'T OF HOMELAND SEC., https://www.dhs.gov/commercial-facilities-sector# (last visited Aug. 23, 2018).

have been in the past, they do not pose a continuous civilian threat like an attack on a country's electric grid or water supply.

Furthermore, this new definition would neither be a replacement of existing definitions of critical infrastructure nor affect nation-states' abilities to expand their own definitions. Rather, it would act as an overarching, supplemental definition, in a vein similar to the European Union's structure for critical infrastructure protection. Each Member State is responsible for its own critical infrastructure, but the European Union has created overarching standards.[103] While each Member State must establish defensive measures for its own critical infrastructure, the European Union has established minimum standards of conduct for those instances where a system disruption would substantially affect more than one Member State.[104] Applying a similar idea to a definition of critical infrastructure and using the goals of the 1949 Geneva Conventions, this single definition can be designed and used in future international agreements.

CONCLUSION

Critical infrastructure is a catchphrase that has been bandied about since the mid-1990s. It is a term that is used frequently and is not always well-defined. Throughout history, nation-states have developed and protected systems that they have found vital to their survival and success. The definition of what is critical, however, has not remained static through time; rather, it has evolved as needs and technologies have changed. Now the world is at a turning point. Society has progressed, and technology has become so advanced that vital systems are reliant on one another and nation-states are dependent on each other. Perhaps even more alarming is that the threat is no longer visible. As Oren Gross states, "[c]omputer networks and information and communication technologies constitute the nerve system of modern society,"[105] and these technologies now control, if not make up, the critical infrastructures of many nation-states. These systems are vulnerable to attack and are easily manipulated; perpetrators can

103. *See generally* Council Directive 2008/114/EC, of the Council of the European Union of 8 Dec. 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection, 2008 O.J. (L 345) 75 (detailing the procedures for setting standards for critical infrastructure within Member States and the European Union).

104. *See generally id.*; *see also* Izuakor & White, *supra* note 96, at 29 (discussing the European Programme for Critical Infrastructure Protection guidelines for fulfilling the requirements of the European Council Directives).

105. *See* Gross, *supra* note 88 at 481.

devastate a country's civilian population with a few keystrokes while oceans away.

These new threat vectors have brought the international community together to establish new rules of engagement in an effort of protecting vital systems of nation-states. However, because those systems that constitute critical infrastructure and priorities differ throughout the world, a new, singular definition of what comprises critical infrastructure is warranted. Thus, rather than extend protections to an ever-changing and inconsistent framework of systems, the international community should redefine and establish an overarching definition to protect civilians from threats that could cause immediate and continuing devastation.